Binary Hamming codes and Boolean designs[1] [2][3]

Giovanni Falcone
Corresponding author
Dipartimento di Matematica e Informatica
Università degli Studi di Palermo, Via Archirafi 34, 90123 Palermo, Italy
giovanni.falcone@unipa.it

Marco Pavone
Dipartimento di Ingegneria
Università degli Studi di Palermo, Viale delle Scienze, 90128 Palermo, Italy
marco.pavone@unipa.it

Abstract

In this paper we consider a finite-dimensional vector space $\mathcal{P}$ over the Galois field GF(2), and the family $\mathcal{B}_k$ (respectively, $\mathcal{B}_k^*$) of all the k-sets of elements of $\mathcal{P}$ (respectively, of $\mathcal{P}^* = \mathcal{P} \setminus \{0\}$) summing up to zero. We compute the parameters of the 3-design $(\mathcal{P}, \mathcal{B}_k)$ for any (necessarily even) k, and of the 2-design $(\mathcal{P}^*, \mathcal{B}_k^*)$ for any k. Also, we find a new proof for the weight distribution of the binary Hamming code.

Moreover, we find the automorphism groups of the above designs by characterizing the permutations of $\mathcal{P}$, respectively of $\mathcal{P}^*$, that induce permutations of $\mathcal{B}_k$, respectively of $\mathcal{B}_k^*$. In particular, this allows one to relax the definitions of the permutation automorphism groups of the binary Hamming code and of the extended binary Hamming code as the groups of permutations that preserve just the codewords of a given Hamming weight.

1 Introduction

Point-flat designs $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ of an affine geometry $\mathrm{AG}(n, p)$ over $\mathrm{GF}(p)$, as well as of a projective geometry $\mathrm{PG}(n, 2)$ over $\mathrm{GF}(2)$, are basic examples of 2-(v, k, λ) designs, and the blocks have the property that the sum of their points is zero. More generally, the so-called 2-(v, k, λ) designs over $\mathrm{GF}(2)$, when seen as 2-$(2^v - 1, 2^k - 1, \lambda)$ designs, whose points are the non-zero vectors of $\mathrm{GF}(2)^v$ and whose blocks are the sets of non-zero vectors of suitable k-dimensional subspaces, form a remarkable class of designs, whose blocks have the property that the sum of their points is zero.

In [10] and [11] it is shown that symmetric and affine 2-designs $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ can be embedded in a finite commutative group in such a way that the blocks are exactly the k-sets of elements of $\mathcal{P}$ that sum up to zero, whereas the only Steiner triple systems with this property are the point-line designs of $\mathrm{AG}(n, 3)$ and $\mathrm{PG}(n, 2)$ (see also [15], for a visual representation of the case of $\mathrm{PG}(3, 2)$). Furthermore, the only known Steiner 2-design over a finite field, found by Braun et al. [5] and revisited in [8], can be seen as a 2-$(8191, 7, 1)$ design with the property that the points on each block sum up to zero. Also, the designs over $\mathrm{GF}(2)$ considered in [7], [28] are 2-$(2^v - 1, 7, 7)$ designs, whose blocks have the property that the sum of their points is zero.

This leads to the following two questions. First, one may ask what 2-designs are *additive*, that is, can be embedded in a finite commutative group $(\mathcal{P}, +)$ in such a way that the sum of the elements in any block is zero [10]. Conversely, let $(\mathcal{P}, +)$ be a finite commutative group

[1] This research was supported by Università di Palermo (FFR).
[2] AMS MSC2020 05B05, 94B05, 51E22.
[3] *Keywords*: Block designs, Hamming codes, permutation automorphisms, weight distribution, subset sum problem.

with v elements, and let $\mathcal{B}_k$ be the family of all the k-sets of elements of $\mathcal{P}$ summing up to zero. One may ask under what conditions the k-sets in $\mathcal{B}_k$ form the blocks of a 2-(v,k,λ) design $\mathcal{D}_k = (\mathcal{P}, \mathcal{B}_k)$. Alternatively, one may consider the family $\mathcal{B}_k^*$ of all the subsets of $\mathcal{P}^*$ of size k whose elements sum up to zero, where $\mathcal{P}^*$ is the set of non-zero vectors in $\mathcal{P}$. The families $\mathcal{B}_k$ and $\mathcal{B}_k^*$ have appeared also in the context of additive combinatorics and additive number theory, in connection with the subset sum problem over finite abelian groups [23].

For $k = 3$, it is easy to see that $\mathcal{D}_3$ is a 2-$(v, 3, \lambda)$ design (necessarily with $\lambda = 1$) if and only if $\mathcal{P}$ is an elementary abelian 3-group. For $k = 4$ and $k = 5$, the following is true (see [9]):

i) $\mathcal{D}_4 = (\mathcal{P}, \mathcal{B}_4)$ is a 2-$(v, 4, \lambda)$ design if and only if $\mathcal{P}$ is an elementary abelian 2-group. In this case, $\lambda = \frac{v-2}{2}$ and, moreover, $\mathcal{D}_4$ is a 3-$(v, 4, 1)$ design;

ii) $\mathcal{D}_5 = (\mathcal{P}, \mathcal{B}_5)$ is a 2-$(v, 5, \lambda)$ design if and only if $\mathcal{P}$ is an elementary abelian 5-group. In this case, $\lambda = \frac{v-3}{2} + \frac{(v-7)\cdot(v-5)}{6}$.

In [25] it is shown that, for an odd prime p, and for $\mathcal{P} = \mathrm{GF}(p)^n$, the incidence structure $\mathcal{D}_k = (\mathcal{P}, \mathcal{B}_k)$ is a 2-(p^n, k, λ) design if and only if k is a multiple of p. In this case,

$$\lambda = \frac{1}{p^n}\binom{p^n - 2}{k-2} + \frac{k-1}{p^n}\binom{p^{n-1} - 1}{k/p - 1}.$$

Moreover, it is shown that the incidence structure $\mathcal{D}_k^* = (\mathcal{P}^*, \mathcal{B}_k^*)$ is a 1-$(p^n - 1, k, r)$ design for any $k \notin \{1, p^n - 2\}$. In either case, the full automorphism group of the design is found, on the basis of the results given in [16]. The question is still open whether $\mathcal{D}_k = (\mathcal{P}, \mathcal{B}_k)$ is a 2-(v, k, λ) design only if $\mathcal{P}$ is an elementary abelian group.

For $p = 2$, and $\mathcal{P} = \mathrm{GF}(2)^n$, the problem shows a somewhat different behaviour and is treated here. In this case, the situation has also been widely studied in the context of coding theory and additive number theory, as the blocks in $\mathcal{B}_k^*$ (respectively, in $\mathcal{B}_k$) can be seen as codewords of weight k in the $(2^n - 1, 2^n - n - 1, 3)$-Hamming code (resp., in the extended binary Hamming code of length 2^n), as well as solutions of the subset sum problem over $\mathrm{GF}(2)^n \setminus \{\mathbf{0}\}$ (resp., over $\mathrm{GF}(2)^n$) in the special case of subsets of size k summing up to 0. For instance, a closed-form expression for the number of blocks in $\mathcal{B}_k^*$ is given in [14, p. 758, Proposition 4.1] (see also [22, Theorem 1.2] in the general case of a prime number p, and the alternative proofs in [23, 21]).

In this self-contained paper we present a collection of results on $\mathcal{D}_k$ and $\mathcal{D}_k^*$ from the point of view of combinatorial design theory. Some of these results were already known merely in the context of coding theory (sometimes only implicitly), whereas some other results are new. In the former case, we provide alternative and purely combinatorial proofs.

In Section 2 we give alternative proofs of the formulas for the cardinalities of the families $\mathcal{B}_k$ and $\mathcal{B}_k^*$, and of the fact that, for k even, $\mathcal{D}_k = (\mathcal{P}, \mathcal{B}_k)$ is a 3-$(2^n, k, \lambda_3)$ design, and we compute the parameter λ_3 explicitly. Also, we give an alternative proof that, for any integer k, with $3 \le k \le 2^n - 4$, $\mathcal{D}_k^* = (\mathcal{P}^*, \mathcal{B}_k^*)$ is a 2-$(2^n - 1, k, \lambda)$ design, and, again, we compute λ explicitly. Finally, we introduce the notion of *indecomposable* blocks in $\mathcal{B}_k^*$, which also define a 2-design, and for which we give a characterization in terms of linear independence, and, independently, in terms of solutions in $\mathcal{P}^*$ of suitable algebraic equations. Any block in $\mathcal{B}_k^*$ is either indecomposable, or the disjoint union of indecomposable blocks of smaller sizes.

In Section 3 we characterize the permutations of $\mathcal{P}$, and $\mathcal{P}^*$, that induce permutations of the families $\mathcal{B}_k$, and $\mathcal{B}_k^*$, respectively, finding a somewhat analogue of the fundamental theorem of affine geometry. This allows us to describe the automorphism groups of the designs $\mathcal{D}_k$ and $\mathcal{D}_k^*$ introduced in Section 2. Moreover, this characterization allows one to relax the definitions of the permutation automorphism groups of the binary Hamming code and of the extended binary Hamming code as the groups of permutations preserving just the codewords of a given Hamming weight (except in the trivial case where the weight equals the length of the code), the former case being somehow known, although never explicitly stated.

2 Boolean designs

Let $\mathcal{P}$ be the n-dimensional vector space $\mathrm{GF}(2)^n$ and let $\mathcal{P}^*$ be the set of non-zero vectors of $\mathcal{P}$. For any positive integer k, we consider the family $\mathcal{B}_k$ of all the k-subsets of $\mathcal{P}$ whose elements sum up to zero, and the family $\mathcal{B}_k^*$ of all the k-subsets of $\mathcal{P}^*$ whose elements sum up to zero. These two families appear at the crossroads between additive combinatorics and algebraic coding theory. Indeed, on the one hand, the k-sets in $\mathcal{B}_k$ and $\mathcal{B}_k^*$ are precisely the solutions of two instances of the well-known *subset sum problem* over finite fields, which arises from a number of relevant applications in combinatorics, coding theory, and graph theory. On the other hand, as we will explain below, the k-sets in $\mathcal{B}_k^*$ (respectively, in $\mathcal{B}_k$) can be seen as codewords of weight k in the binary Hamming code C of length $m = 2^n - 1$ (resp., in the extended binary Hamming code $\bar{C}$ of length 2^n). In this section we will instead look at $\mathcal{B}_k$ and $\mathcal{B}_k^*$ from the point of view of design theory, that is, by taking them as the families of blocks of two *Boolean* combinatorial designs $\mathcal{D}_k$ and $\mathcal{D}_k^*$ with point-sets $\mathcal{P}$ and $\mathcal{P}^*$, respectively, for suitable values of k.

Let C be the binary Hamming code of length $m = 2^n - 1$ ($n \geq 3$), and let H be a parity check matrix for C, that is, an $n \times m$ matrix whose columns are the elements of $\mathcal{P}^*$. Thus C is the kernel of the linear map $X \mapsto HX$ (seen as column vectors) from $\mathrm{GF}(2)^m$ onto $\mathrm{GF}(2)^n$. If we denote, as usual, the i-th column of H by H^i, and if $\{i_1, i_2, \ldots, i_h\}$ is the support of a generic codeword $X = (x_1, x_2, \ldots, x_m)$ in C of weight h, that is, $i_1, \ldots, i_h$ are those coordinates i such that $x_i \neq 0$, with $3 \leq h \leq 2^n - 4$, then the map

$$\theta : (x_1, x_2, \ldots, x_m) \mapsto \{H^{i_1}, H^{i_2}, \ldots, H^{i_h}\} \tag{1}$$

defines a one-to-one correspondence between the codewords of a given weight k in C and the k-sets in $\mathcal{B}_k^*$. In particular, the problem of the so-called weight distribution of C reduces to the computation of the cardinalities of the families $\mathcal{B}_k^*$. It must be noted that for p-ary Hamming codes (p an odd prime) the one-to-one correspondence fails to exist in general, with the only exception of the cases where $p \in \{3, 5\}$ and $k = 3$.

Similarly, the extended binary Hamming code $\bar{C}$ is the code of length $2^n = m + 1$ obtained from C by adding to each codeword $(x_1, x_2, \ldots, x_m)$ an extra "parity bit" x_0, with $x_0 = x_1 + x_2 + \ldots + x_m$, so that all $m + 1$ digits sum up to 0, whence all the codewords $(x_0, x_1, \ldots, x_m)$ in $\bar{C}$ have even weights. If $\mathbf{0}$ denotes the zero vector in $\mathrm{GF}(2)^n$, then the map

$$\bar{\theta} : (x_0, x_1, \ldots, x_m) \mapsto \begin{cases} \theta(x_1, x_2, \ldots, x_m) & \text{if } x_0 = 0 \\ \{\mathbf{0}\} \cup \theta(x_1, x_2, \ldots, x_m) & \text{if } x_0 = 1 \end{cases} \tag{2}$$

defines a one-to-one correspondence between the codewords of a given weight k in $\bar{C}$ and the k-sets in $\mathcal{B}_k$.

In the more general context of a 1-error perfect binary code C of length m, Etzion and Vardy [14, Proposition 4.1] found a closed-form expression for the weight distribution of C, starting from the well-known doubly-recursive relation

$$(m-i+1)A_{i-1} + A_i + (i+1)A_{i+1} = \binom{m}{i} \tag{3}$$

[24, p. 129] (see also [26]), where A_i denotes the number of codewords of weight i in C. Note that the equation (3) has only two possible solutions, depending on whether C contains the zero vector ($A_0 = 1, A_1 = 0$) or not ($A_0 = 0, A_1 = 1$). If $e_1, \ldots, e_m$ are the vectors of the canonical basis of $\mathrm{GF}(2)^m$, then, C being a 1-error perfect code, $\mathrm{GF}(2)^m$ can be partitioned as the disjoint union of the (1-error perfect) codes $C, C + e_1, \ldots, C + e_m$. If C contains the zero vector, then the codes $C + e_1, \ldots, C + e_m$ do not contain it, hence they all share the same weight distribution. Therefore, if B_i denotes the common number of words of weight i in any of the codes $C + e_1, \ldots, C + e_m$, one obtains that $A_i + mB_i = \binom{m}{i}$, which, together with the relation $(m-i+1)A_{i-1} + A_i + (i+1)A_{i+1} = (m-i+1)B_{i-1} + B_i + (i+1)B_{i+1}$, produces by induction an explicit expression for A_i.

Independently, in the context of the subset sum problem, the cardinalities of $\mathcal{B}_k$ and $\mathcal{B}_k^*$ were computed in closed form by Li and Wan [22] in the general case of a finite field $\mathcal{P}$ of characteristic $p \geq 2$. For any b in $\mathcal{P}$, they let $M(k, b, D)$ be the number of ordered k-tuples $(x_1, x_2, \ldots, x_k)$ satisfying $x_1 + x_2 + \ldots + x_k = b$, where D was either $\mathcal{P}$ or $\mathcal{P}^*$ (note that $M(k, 0, \mathcal{P}) = k!\,|\mathcal{B}_k|$ and $M(k, 0, \mathcal{P}^*) = k!\,|\mathcal{B}_k^*|$). They found several recursive relations among the values of $M(k, 0, \mathcal{P})$, $M(k, 0, \mathcal{P}^*)$, $M(k, 1, \mathcal{P})$, and $M(k, 1, \mathcal{P}^*)$, 1 being the identity element of the multiplicative group of the field $\mathcal{P}$, also by considering the p-rank of the coefficient matrix of a suitable system of equations.

In this section, first of all, we give an alternative proof of the formulas for the cardinalities of the families $\mathcal{B}_k$ and $\mathcal{B}_k^*$, which is more immediate than the above mentioned proofs. Subsequently, we show that, for any $n \geq 3$ and any even integer k, with $4 \leq k \leq 2^n - 4$, $\mathcal{B}_k$ is not empty, and give an elementary proof that $\mathcal{D}_k = (\mathcal{P}, \mathcal{B}_k)$ is a 3-$(2^n, k, \lambda_3)$ design. Moreover, we give an explicit expression for λ_3 and determine the automorphism group of $\mathcal{D}_k$. Also, we prove that, for any $n \geq 3$ and any integer k, with $3 \leq k \leq 2^n - 4$, $\mathcal{B}_k^*$ is not empty, and give an elementary proof that $\mathcal{D}_k^* = (\mathcal{P}^*, \mathcal{B}_k^*)$ is a 2-$(2^n - 1, k, \lambda)$ design. Again, we compute λ and determine the automorphism group of $\mathcal{D}_k^*$. Finally, we show that any block in $\mathcal{B}_k^*$ can be partitioned into the disjoint union of *indecomposable* blocks, which turn out to be precisely the k-sets of vectors in $\mathcal{P}^*$, $k-1$ of which are linearly independent.

2.1 Remarks: (*i*) The set $\mathcal{P}^*$ under consideration is a projective space over the field GF(2) and, in particular, $\mathcal{D}_3$ is isomorphic to the point-line design of $\mathrm{PG}(n-1, 2)$.

(*ii*) In the affine space $\mathcal{P} = \mathrm{GF}(2)^n$ a necessary and sufficient condition for four distinct points to be an affine plane is that their sum is zero. Hence the 4-sets in $\mathcal{B}_4$ are precisely the blocks of the classical point-plane design of the affine geometry $\mathrm{AG}(n, 2)$ over GF(2), that is, of the Boolean quadruple system of order 2^n. These have been studied e.g. in [1], [6], [17, Example 2.3], [20] and [29]. For this reason, we will call *Boolean designs*, by extension, the block designs defined in this section, with block-sets $\mathcal{B}_k$ and $\mathcal{B}_k^*$.

We now give a new proof of the closed-form expressions for $|\mathcal{B}_k|$ and $|\mathcal{B}_k^*|$. The idea is very simple, and relies on the immediate observation that $\mathcal{B}_k$ consists of all the k-subsets $\{x_1, \ldots, x_{k-1}, x_1 + \cdots + x_{k-1}\}$ of $\mathcal{P}$ for which $x_1, \ldots, x_{k-1}$ are pairwise different, and $x_1 + \cdots + x_{k-1}$ is different from all the preceding vectors, that is, $\{x_1, \ldots, x_{k-1}\}$ does not contain any $(k-2)$-subset belonging to $\mathcal{B}_{k-2}$. This allows us to get a simply-recursive relation between $|\mathcal{B}_k|$ and $|\mathcal{B}_{k-2}|$, which, by induction, produces the explicit expression for $|\mathcal{B}_k|$. Finally, the expression for $|\mathcal{B}_k^*|$ is also obtained by induction, starting from the trivial observation that $|\mathcal{B}_k^*| = |\mathcal{B}_k| - |\mathcal{B}_{k-1}^*|$.

2.2 Theorem: [22, Theorem 1.2] *Let $\mathcal{P}$ be an n-dimensional vector space over* GF(2), $n \geq 1$. *For any integer k, with $1 \leq k \leq 2^n$, let $\mathcal{B}_k$ be the family of all the subsets of $\mathcal{P}$ of size k whose elements sum up to zero. If we denote $|\mathcal{B}_k|$ by b_k, then*

$$b_k = \begin{cases} \dfrac{1}{2^n}\dbinom{2^n}{k} & \text{if } k \text{ is odd} \\ \dfrac{1}{2^n}\dbinom{2^n}{k} + (-1)^{k/2}\,\dfrac{2^n-1}{2^n}\dbinom{2^{n-1}}{k/2} & \text{if } k \text{ is even.} \end{cases} \tag{4}$$

Proof. For $k = 1$, $\mathcal{B}_k = \{(0, \ldots, 0)\}$ and $b_k = 1$, whereas, for $k = 2$, $\mathcal{B}_k = \emptyset$ and $b_k = 0$. In either case, the equality (4) is satisfied. We may then assume that $k \geq 3$. Let A be the family of $(k-1)$-subsets of $\mathcal{P}$ defined by

$$A = \left\{ \{x_1, x_2, \ldots, x_{k-1}\} \in \binom{\mathcal{P}}{k-1} \Big| \sum_{i \neq j} x_i \neq (0, \ldots, 0) \text{ for all } j = 1, 2, \ldots, k-1 \right\},$$

and let $\tau : A \to \mathcal{B}_k$ be the map defined by

$$\tau(\{x_1, x_2, \ldots, x_{k-1}\}) = \{x_1, x_2, \ldots, x_{k-1}, x_1 + x_2 + \ldots + x_{k-1}\}.$$

Now τ is surjective and

$$\tau^{-1}(\{y_1, \ldots, y_k\}) = \big\{ \{y_1, \ldots, y_k\} \setminus \{y_i\} \big| \, i = 1, 2, \ldots, k \big\}$$

for all $\{y_1, \ldots, y_k\} \in \mathcal{B}_k$, hence

$$b_k = \frac{1}{k}\,|A|. \tag{5}$$

On the other hand,

$$A = \binom{\mathcal{P}}{k-1} \setminus \left\{ \{x_1, x_2, \ldots, x_{k-1}\} \in \binom{\mathcal{P}}{k-1} \Big| \sum_{i \neq j} x_i = (0, \ldots, 0) \text{ for some } 1 \leq j \leq k-1 \right\},$$

hence, by (5),

$$b_k = \frac{1}{k}\left(\binom{2^n}{k-1} - \big(2^n - (k-2)\big)\, b_{k-2} \right). \tag{6}$$

We can now proceed by induction. If k is odd, then $k-2$ is also odd, hence, by (6) and (4) (with subscript $k-2$),

$$\begin{aligned} b_k &= \frac{1}{k}\left(\binom{2^n}{k-1} - \big(2^n-(k-2)\big)\,\frac{1}{2^n}\binom{2^n}{k-2}\right) \\ &= \frac{1}{k}\left(\binom{2^n}{k-1} - \frac{k-1}{2^n}\binom{2^n}{k-1}\right) \\ &= \frac{1}{k}\binom{2^n}{k-1}\,\frac{2^n-(k-1)}{2^n} \\ &= \frac{1}{2^n}\binom{2^n}{k}. \end{aligned}$$

If k is even, say $k=2m$, then $k-2=2(m-1)$, hence, by (6) and (4) (with subscript $k-2$),

$$\begin{aligned} b_k &= \frac{1}{k}\binom{2^n}{k-1} - \frac{2^n-(k-2)}{k}\left(\frac{1}{2^n}\binom{2^n}{k-2} + (-1)^{m-1}\,\frac{2^n-1}{2^n}\binom{2^{n-1}}{m-1}\right) \\ &= \frac{1}{k}\binom{2^n}{k-1} - \frac{k-1}{k\,2^n}\binom{2^n}{k-1} + (-1)^m\,\frac{2^{n-1}-(m-1)}{m}\,\frac{2^n-1}{2^n}\binom{2^{n-1}}{m-1} \\ &= \frac{2^n-(k-1)}{k\,2^n}\binom{2^n}{k-1} + (-1)^m\,\frac{2^n-1}{2^n}\binom{2^{n-1}}{m} \\ &= \frac{1}{2^n}\binom{2^n}{k} + (-1)^m\,\frac{2^n-1}{2^n}\binom{2^{n-1}}{m}. \end{aligned}$$

Alternatively, the equality $b_k = \frac{1}{2^n}\binom{2^n}{k}$ for k odd can be immediately obtained by noting that

$$\binom{\mathcal{P}}{k} = \bigcup_{x\in\mathcal{P}} \left\{ \{x_1,x_2,\ldots,x_k\} \in \binom{\mathcal{P}}{k} \Big|\ \sum_{i=1}^{k} x_i = x \right\},$$

and that, for each $x\in\mathcal{P}$, the map $\{x_1,x_2,\ldots,x_k\} \mapsto \{x_1+x, x_2+x, \ldots, x_k+x\}$ is a one-to-one correspondence between $\mathcal{B}_k$ and the family $\big\{\{x_1,x_2,\ldots,x_k\} \in \binom{\mathcal{P}}{k} \big|\ \sum_{i=1}^{k} x_i = x\big\}$.

This completes the proof of the theorem. □

2.3 Lemma: *Let $\mathcal{P}$ be an n-dimensional vector space over* GF(2), *$n\geq 1$, and let $\mathcal{P}^* = \mathcal{P}\setminus\{0\}$. For any integer k, let $\mathcal{B}_k$ (respectively, $\mathcal{B}_k^*$) be the family of all the subsets of $\mathcal{P}$ (resp., of $\mathcal{P}^*$) of size k whose elements sum up to zero. If we denote $|\mathcal{B}_k|$ by b_k, and $|\mathcal{B}_k^*|$ by b_k^*, then, for any $k=2,\ldots,2^n-1$,*

$$b_k^* = b_k - b_{k-1}^*. \tag{7}$$

Proof. For any $k=2,\ldots,2^n-1$, $\mathcal{B}_k$ is the (possibly empty) disjoint union of $\mathcal{B}_k^*$ with the family of all the subsets of $\mathcal{P}$ of size k containing zero, whose elements sum up to zero. As the latter family is in one-to-one correspondence with $\mathcal{B}_{k-1}^*$, the equality follows. □

In the following result we derive an explicit expression for the cardinality of the family $\mathcal{B}_k^*$, which, because of the correspondence (1), also gives the weight distribution of the binary Hamming code.

2.4 Corollary: [14, Proposition 4.1][22, Theorem 1.2] *Let $\mathcal{P}$ be an n-dimensional vector space over* GF(2), $n \geq 1$, *and let $\mathcal{P}^* = \mathcal{P} \setminus \{0\}$. For any integer $k = 1, \ldots, 2^n - 1$, let $\mathcal{B}_k^*$ be the family of all the subsets of $\mathcal{P}^*$ of size k whose elements sum up to zero. If we denote $|\mathcal{B}_k^*|$ by b_k^*, then, for any $k = 1, \ldots, 2^n - 1$,*

$$b_k^* = \frac{1}{2^n}\binom{2^n - 1}{k} + (-1)^{k+\lfloor k/2 \rfloor}\ \frac{2^n - 1}{2^n}\binom{2^{n-1} - 1}{\lfloor k/2 \rfloor}, \tag{8}$$

where $\lfloor \cdot \rfloor$ is the floor function.

Proof. For $k = 1$, the equality is trivial. For $2 \leq k \leq 2^n - 1$, we can proceed by induction. If k is odd, say $k = 2m + 1$, then $\lfloor k/2 \rfloor = m$, $k - 1 = 2m$ and, by (7), (4), and (8) (with subscript $k - 1$),

$$\begin{aligned} b_k^* &= \frac{1}{2^n}\binom{2^n}{k} - \left(\frac{1}{2^n}\binom{2^n - 1}{k-1} + (-1)^{3m}\ \frac{2^n - 1}{2^n}\binom{2^{n-1} - 1}{m}\right) \\ &= \frac{1}{2^n}\binom{2^n - 1}{k} + (-1)^{3m+1}\ \frac{2^n - 1}{2^n}\binom{2^{n-1} - 1}{m}, \end{aligned}$$

that is, (8) holds. If k is even, say $k = 2m$, then $\lfloor k/2 \rfloor = m$, $k-1 = 2m-1$, $\lfloor (k-1)/2 \rfloor = m-1$, and, by (7), (4), and (8) (with subscript $k - 1$),

$$\begin{aligned} b_k^* &= \frac{1}{2^n}\binom{2^n}{k} + (-1)^m\ \frac{2^n - 1}{2^n}\binom{2^{n-1}}{m} - \left(\frac{1}{2^n}\binom{2^n - 1}{k-1} + (-1)^{3m}\ \frac{2^n - 1}{2^n}\binom{2^{n-1} - 1}{m-1}\right) \\ &= \frac{1}{2^n}\binom{2^n - 1}{k} + (-1)^{3m}\ \frac{2^n - 1}{2^n}\binom{2^{n-1} - 1}{m}, \end{aligned}$$

that is, (8) holds. The proof is now complete. □

In [3, Theorem 3], the authors prove that for any extended 1-perfect code containing $\mathbf{0}$, the codewords of a given weight form a $(d - s + 1)$-design, where d is the minimal distance and s is the covering radius. In particular, when the code is an extended binary Hamming code, this yields that the codewords of a given weight form a 3-design. In what follows, after providing an elementary proof of the previous statement, we find the value of the parameter λ_3, and the isomorphism $\mathrm{Aut}(\mathcal{D}_k) \simeq \mathrm{Aff}(n, 2)$, which, in the light of the subsequent Theorem 3.2.ii, also gives an alternative proof of the permutation automorphisms of the extended binary Hamming code as the invertible affine mappings on $\mathcal{P}$ over GF(2).

2.5 Proposition: *Let $\mathcal{P}$ be an n-dimensional vector space over* GF(2), $n \geq 3$. *For any even $k = 2m$, with $4 \leq k \leq 2^n - 4$, let $\mathcal{B}_k$ be the family of all the subsets of $\mathcal{P}$ of size k whose elements sum up to zero. Then $\mathcal{B}_k$ is not empty, and $\mathcal{D}_k = (\mathcal{P}, \mathcal{B}_k)$ is a 3-$(2^n, k, \lambda_3)$ design, with*

$$\lambda_3 = \frac{1}{2^n}\binom{2^n - 3}{k - 3} + (-1)^{k/2}\ \frac{k - 1}{2^n}\binom{2^{n-1} - 2}{\frac{k}{2} - 2}.$$

Moreover, the group of automorphisms of $\mathcal{D}_k$ is (isomorphic to) the group of invertible affine mappings on $\mathcal{P}$ over GF(2), *that is,*

$$\mathrm{Aut}(\mathcal{D}_k) \simeq \mathrm{Aff}(n,2).$$

Proof. Let us first show that the family $\mathcal{B}_k$ is not empty. Even though this can be settled by use of the formula (4) for the cardinality of $\mathcal{B}_k$, we will now give a direct proof in a few lines. As the sum of all the 2^n elements of $\mathcal{P}$ is equal to zero, we may assume, up to taking complements, that $k \leq 2^{n-1}$. Note that each plane $S = \{a, a+x, a+y, a+x+y\}$ in $\mathcal{P}$ has the property that the sum of its elements is zero. If m is even, say $m = 2h$, then $k = 4h$, and any disjoint union of h planes is in $\mathcal{B}_k$. If m is odd, say $m = 2h+1$, $1 \leq h \leq 2^{n-3}-1$, then $k = 6+4(h-1)$. If $\{e_1, e_2, \ldots, e_n\}$ is the canonical basis of $\mathcal{P}$, then the linear span V of $e_1, e_2, \ldots, e_{n-1}$ is the disjoint union of 2^{n-3} planes. Hence the union $\left(\bigcup_{i=1}^{h-1}(S_i + e_n)\right) \bigcup \{e_1, e_2, e_3, e_4, e_1+e_2, e_3+e_4\}$, where $S_1, \ldots, S_{h-1}$ are disjoint planes in V, is a k-set in $\mathcal{B}_k$.

Let $\{P_1, P_2, P_3\}$ and $\{Q_1, Q_2, Q_3\}$ be two 3-subsets of $\mathcal{P}$. Since the group of affinities of $\mathcal{P}$ acts 3-transitively on $\mathcal{P}$, there exists an affinity $\rho : X \mapsto AX + B$ such that $\rho(P_i) = Q_i$, $i = 1, 2, 3$. For any given $\mathfrak{b} \in \mathcal{B}_k$,

$$\sum_{Q \in \rho(\mathfrak{b})} Q = \sum_{X \in \mathfrak{b}} (AX + B) = k\, B = 0,$$

since k is even, thus $\rho(\mathfrak{b})$ is in $\mathcal{B}_k$. Hence ρ induces a one-to-one correspondence between the k-sets in $\mathcal{B}_k$ containing P_1, P_2, P_3 and the k-sets in $\mathcal{B}_k$ containing Q_1, Q_2, Q_3. Therefore $\mathcal{D}_k$ is a 3-$(2^n, k, \lambda_3)$ design. In particular, $\mathcal{D}_k$ is also a 2-design with $\lambda_2 = \lambda_3 \frac{2^n-2}{k-2}$. On the other hand, $\lambda_2(2^n-1) = r(k-1)$, where $r = k\, b_k/2^n$, with $b_k = |\mathcal{B}_k|$. By Theorem 2.2, we may conclude that

$$\begin{aligned}
\lambda_3 &= \frac{k}{2^n}\,\frac{k-1}{2^n-1}\,\frac{k-2}{2^n-2}\,b_k \\
&= \frac{k}{2^n}\,\frac{k-1}{2^n-1}\,\frac{k-2}{2^n-2}\left(\frac{1}{2^n}\binom{2^n}{k} + (-1)^m\,\frac{2^n-1}{2^n}\binom{2^{n-1}}{m}\right) \\
&= \frac{1}{2^n}\binom{2^n-3}{k-3} + (-1)^m\,\frac{k}{2^n}\,\frac{k-1}{2^n-1}\,\frac{k-2}{2^n-2}\,\frac{2^n-1}{2^n}\,\frac{2^{n-1}}{m}\,\frac{2^{n-1}-1}{m-1}\binom{2^{n-1}-2}{m-2} \\
&= \frac{1}{2^n}\binom{2^n-3}{k-3} + (-1)^m\,\frac{k-1}{2^n}\binom{2^{n-1}-2}{m-2}.
\end{aligned}$$

The final statement on the automorphisms is a consequence of the subsequent Theorem 3.2.ii.

This completes the proof. □

In [13, Theorem 5.7], the author proves that for any 1-perfect code containing $\mathbf{0}$, the codewords of a given weight form a $(d-s)$-design, where d is the minimal distance and s is the covering radius. In particular, when the code is a binary Hamming code, this yields that the codewords of a given weight form a 2-design. In what follows, we give an elementary proof of the previous statement and find the value of the parameter λ and the isomorphism

$\mathrm{Aut}(\mathcal{D}_k^*) \simeq \mathrm{GL}(n,2)$, which, in the light of the subsequent Theorem 3.1, also provides an independent proof of the permutation automorphisms of the binary Hamming code as the invertible linear mappings on $\mathcal{P}$ over GF(2).

2.6 Proposition: *Let $\mathcal{P}$ be an n-dimensional vector space over* GF(2), $n \geq 3$. *For any integer k, with $3 \leq k \leq 2^n - 4$, let $\mathcal{B}_k^*$ be the family of all the subsets of $\mathcal{P}^*$ of size k whose elements sum up to zero. Then $\mathcal{B}_k^*$ is not empty, and $\mathcal{D}_k^* = (\mathcal{P}^*, \mathcal{B}_k^*)$ is a 2-$(2^n - 1, k, \lambda)$ design, with*

$$\lambda = \frac{1}{2^n}\binom{2^n-3}{k-2} + (-1)^{k+\lfloor k/2 \rfloor}\ \frac{1}{2^n}\ \frac{(k-1)k}{2\lfloor k/2 \rfloor}\ \binom{2^{n-1}-2}{\lfloor k/2 \rfloor - 1}.$$

Moreover, the group of automorphisms of $\mathcal{D}_k^*$ is (isomorphic to) the group of invertible linear mappings on $\mathcal{P}$ over GF(2), *that is,*

$$\mathrm{Aut}(\mathcal{D}_k^*) \simeq \mathrm{GL}(n,2).$$

Proof. Let us first show that the family $\mathcal{B}_k^*$ is not empty. Again, we will give a direct proof, independently of the equality (8). If k is odd, with $3 \leq k \leq 2^n - 5$, then $k+1$ is even, and $4 \leq k+1 \leq 2^n - 4$, whence $\mathcal{B}_{k+1}$ is not empty by Proposition 2.5. Thus $\mathcal{B}_k^*$ is not empty, as $(\mathcal{P}^*, \mathcal{B}_k^*)$ is the derived design at 0 of the design $(\mathcal{P}, \mathcal{B}_{k+1})$. If k is even, with $4 \leq k \leq 2^n - 4$, then let r be the replication number of the 3-$(2^n, k, \lambda_3)$ design $(\mathcal{P}, \mathcal{B}_k)$, where $\mathcal{B}_k$ is not empty by Proposition 2.5. Now $2^n r = k\, b_k$ and $k < 2^n$, hence $r < b_k$. Since $\mathcal{B}_k^* = \mathcal{B}_k \setminus \{\mathfrak{b} \in \mathcal{B}_k \,|\, 0 \in \mathfrak{b}\}$, we conclude that $|\mathcal{B}_k^*| = b_k - r > 0$, as claimed.

Let $\{P_1, P_2\}$ and $\{Q_1, Q_2\}$ be two 2-subsets of $\mathcal{P}^*$. Then P_1 and P_2 are linearly independent over GF(2), as well as Q_1 and Q_2. Hence there exists an invertible linear map ρ on $\mathcal{P}$ over GF(2) such that $\rho(P_i) = Q_i$, $i = 1, 2$. For any given $\mathfrak{b} \in \mathcal{B}_k^*$, $\rho(\mathfrak{b})$ is trivially in $\mathcal{B}_k^*$, hence ρ induces a one-to-one correspondence between the k-sets in $\mathcal{B}_k^*$ containing P_1, P_2 and the k-sets in $\mathcal{B}_k^*$ containing Q_1, Q_2. Therefore $\mathcal{D}_k^*$ is a 2-$(2^n - 1, k, \lambda)$ design.

By the basic relations on the parameters of a 2-design, $\lambda(2^n - 2) = r(k-1)$, where $r = k\, b_k^*/(2^n - 1)$, with $b_k^* = |\mathcal{B}_k^*|$. By Corollary 2.4, we may conclude that

$$\begin{aligned}
\lambda &= \frac{k-1}{2^n-2}\,\frac{k}{2^n-1}\,b_k^* \\
&= \frac{k-1}{2^n-2}\,\frac{k}{2^n-1}\left(\frac{1}{2^n}\binom{2^n-1}{k} + (-1)^{k+\lfloor k/2 \rfloor}\ \frac{2^n-1}{2^n}\binom{2^{n-1}-1}{\lfloor k/2 \rfloor}\right) \\
&= \frac{1}{2^n}\binom{2^n-3}{k-2} + (-1)^{k+\lfloor k/2 \rfloor}\ \frac{k-1}{2^n-2}\,\frac{k}{2^n}\,\frac{2^{n-1}-1}{\lfloor k/2 \rfloor}\,\binom{2^{n-1}-2}{\lfloor k/2 \rfloor - 1} \\
&= \frac{1}{2^n}\binom{2^n-3}{k-2} + (-1)^{k+\lfloor k/2 \rfloor}\ \frac{1}{2^n}\ \frac{(k-1)k}{2\lfloor k/2 \rfloor}\ \binom{2^{n-1}-2}{\lfloor k/2 \rfloor - 1}.
\end{aligned}$$

An alternative way to prove this formula can be obtained by resorting again to the fact that $(\mathcal{P}^*, \mathcal{B}_k^*)$ is the derived design at 0 of the design $(\mathcal{P}, \mathcal{B}_{k+1})$. If k is odd, then $k+1$ is even, and for any pair of distinct points x, y in $\mathcal{P}^*$, the number of blocks in $\mathcal{B}_k^*$ through x and y is equal

to the number of blocks in $\mathcal{B}_{k+1}$ through 0, x, and y in the 3-$(2^n, k+1, \lambda_3)$ design $(\mathcal{P}, \mathcal{B}_{k+1})$, hence $\lambda = \lambda_3$ can be computed by means of Proposition 2.5.

If k is even, then note that the design $\mathcal{D}_k^*$ is the point residue of $\mathcal{D}_k$ with respect to 0 [4, Remark 1.8, p. 64]. Let λ_2 be the constant number of blocks through any two distinct points in the 3-$(2^n, k, \lambda_3)$ design $(\mathcal{P}, \mathcal{B}_k)$. Now, for any pair of distinct points x, y in $\mathcal{P}^*$, the family of blocks in $\mathcal{B}_k$ through x and y is the disjoint union of the family of blocks in $\mathcal{B}_k$ through 0, x, and y and the family of blocks in $\mathcal{B}_k$ through x and y not containing 0, where, in turn, the latter family has the same cardinality as the family of blocks in $\mathcal{B}_k^*$ through x and y. Hence $\lambda = \lambda_2 - \lambda_3$, and, again, λ can be computed by means of Proposition 2.5. The reader may check that, in either case, the formula for λ coincides with that given above.

The final statement on the automorphisms is a consequence of the subsequent Theorem 3.1. This completes the proof. □

2.7 Remarks: 1) For k odd, $1 \le k \le 2^n - 1$, $\mathcal{D}_k = (\mathcal{P}, \mathcal{B}_k)$ is not even a 1-design. Indeed, let x be a point in $\mathcal{P}$, and let $r_k(x)$ be the cardinality of the family of all the k-sets in $\mathcal{B}_k$ containing x. Now, the map $\{x, x_2, \ldots, x_k\} \mapsto \{x_2 + x, \ldots, x_k + x\}$ is a one-to-one correspondence between the latter family and the family of all the $(k-1)$-subsets of $\mathcal{P}^*$ whose elements sum up to x. Hence, following the notation used in [22],

$$r_k(x) = N(k-1, x, \mathcal{P}^*).$$

Therefore, by Theorem 1.2 in [22], $r_k(y) \neq r_k(0)$ for all $y \neq 0$. Hence $r_k(x)$ is not constant in x, that is, $\mathcal{D}_k$ is not a 1-design.

2) For k even, the 3-$(2^n, k, \lambda_3)$ design $\mathcal{D}_k = (\mathcal{P}, \mathcal{B}_k)$ is not, in general, a 4-design. As mentioned above in Remark 2.1(ii), for $k = 4$ the blocks of $\mathcal{D}_4$ are precisely the affine planes of $\mathcal{P}$, thus there exists exactly one block through any four coplanar distinct points, whereas there is no block through four distinct points not in a plane. For $k = 6$, there exists no block through four coplanar distinct points (as their sum is zero), whereas any four linearly independent vectors in $\mathcal{P}$ can be completed to a block of $\mathcal{D}_6$ by adding $\mathbf{0}$ and their sum. The general case of an even $k \ge 8$ appears hard enough not to be settled here.

Similarly, the 2-$(2^n - 1, k, \lambda)$-design $\mathcal{D}_k^*$ is not necessarily a 3-design.

3) By construction, the block designs $\mathcal{D}_k$ and $\mathcal{D}_k^*$ have the property that they can be embedded in a commutative group $(G, +)$ in such a way that a sufficient and necessary condition for a k-subset of the point-set to be a block is that the sum of its elements is zero in G. The same is true for all the designs found in [10, 11, 25]. In particular, they are *additive* in the sense of the definition given in [10], and it is an open problem whether the property above is sufficient for any additive 2-design [11, 3.10].

4) It is worth noting that a class of (additive) subdesigns of the Boolean design $\mathcal{D}_{2^k-1}^*$ is given by the 2-(v, k, λ) designs over GF(2), when seen as 2-$(2^v - 1, 2^k - 1, \lambda)$ designs.

5) For $n = 3$ and $k = 3$ (respectively, $k = 4$) the design in Proposition 2.6 is a 2-$(7, 3, 1)$ design (resp. a 2-$(7, 4, 2)$ design), that is, it is the Fano plane (resp. the unique biplane of order 2). The two designs are the complementary design of one another, and it is well known that the automorphism group of the two designs is (isomorphic to) GL$(3, 2)$, consistently with Proposition 2.6. More generally, for $k = 3$, the design $(\mathcal{P}^*, \mathcal{B}_3^*)$ is a 2-$(2^n - 1, 3, 1)$ design, that is, a Steiner triple system of order $2^n - 1$, which, as we noted at the beginning of this section, is

isomorphic to the Steiner triple system of all the codewords of weight 3 in the binary Hamming code of length $2^n - 1$.

6) As we mentioned earlier in this section, for $k = 4$ the design $\mathcal{D}_4$ in the above Proposition 2.5 is the Boolean quadruple system of order 2^n [17, Example 2.3], that is, the classical point-plane design of the affine geometry $\mathrm{AG}(n, 2)$ over $\mathrm{GF}(2)$, which is a 3-$(2^n, 4, 1)$ Steiner quadruple system. In this case, the action of the group of affinities of $\mathcal{P}$ on the 4-subsets of $\mathcal{P}$ has precisely two orbits, $\mathcal{B}_4$ and $\binom{\mathcal{P}}{4} \setminus \mathcal{B}_4$, hence $\mathcal{D}_4$ and its complementary design are special cases of the t-designs constructed in [12, Remark 4.29]. As the blocks of $\mathcal{B}_4$ are exactly the affine planes of $\mathcal{P}$, one may ask whether in general, for k even, any block of $\mathcal{B}_k$ consists of the disjoint union of affine subspaces.

For $k = 6$ (hence $n \geq 4$) we see that a block, e.g. the 6-set consisting of the zero vector, four vectors of the canonical basis, and the sum of all of them, cannot be either an affine subspace nor the disjoint union of a plane and a line. On the other hand, each pair of distinct points being a line, a block is (in 15 different ways) the disjoint union of three lines (but, clearly, not any disjoint union of three lines is a block).

Consider now the case where $k = 8$ (and $n \geq 4$). It is easy to see that, in the affine spaces $\mathrm{GF}(2)^4$ and $\mathrm{GF}(2)^5$, a necessary and sufficient condition for eight distinct points to lie in two disjoint planes is that their sum is zero. Hence the design we get for $k = 8$, and $n = 4, 5$, is the design of disjoint pairs of two-dimensional (affine) subspaces of an affine space over $\mathrm{GF}(2)$. Things change for $\mathrm{GF}(2)^6$, because the 8-set consisting of the zero vector, the six vectors of the canonical basis, and the sum of all of them, cannot be described as the disjoint union of two affine subplanes.

The last remark above suggests the following definition, which concerns necessarily blocks in $\mathcal{B}_k^*$, since the zero vector would make decomposable any block containing it.

2.8 Definition: *Let $(\mathcal{P}^*, \mathcal{B}_k^*)$ be the above 2-$(2^n-1, k, \lambda)$ design, with $n \geq 3$ and $3 \leq k \leq 2^n-4$. We say that a block $\mathfrak{b} \in \mathcal{B}_k^*$ is* decomposable *if it is the union of two disjoint blocks $\mathfrak{b}_1 \in \mathcal{B}_{k_1}^*$, $\mathfrak{b}_2 \in \mathcal{B}_{k_2}^*$ of the designs $(\mathcal{P}^*, \mathcal{B}_{k_1}^*)$, $(\mathcal{P}^*, \mathcal{B}_{k_2}^*)$, where $k_1 + k_2 = k$. We say that a block $\mathfrak{b} \in \mathcal{B}_k^*$ is* indecomposable *if it is not decomposable.*

2.9 Theorem: *Let $(\mathcal{P}^*, \mathcal{B}_k^*)$ be the above 2-$(2^n-1, k, \lambda)$ design, with $n \geq 3$ and $3 \leq k \leq 2^n-4$. A block $\mathfrak{b} \in \mathcal{B}_k^*$ is indecomposable if and only if $\mathfrak{b}$ contains $k-1$ linearly independent vectors, i.e., if and only if $3 \leq k \leq n+1$ and $\mathfrak{b}$ is contained in the orbit of*

$$\mathfrak{c}_k = \{e_1, \ldots, e_{k-1}, e_1 + e_2 + \cdots + e_{k-1}\}$$

under $\mathrm{GL}(n, 2)$, where $\{e_1, \ldots, e_n\}$ is the canonical basis of $\mathcal{P} = \mathrm{GF}(2)^n$.

Also, for $3 \leq k \leq n+1$, the family of indecomposable blocks in $\mathcal{B}_k^*$ defines a 2-$(2^n - 1, k, \tilde{\lambda})$ design, where

$$\tilde{\lambda} = \begin{cases} 1 & \text{if } k = 3 \\ \dfrac{(2^n-4)(2^n-8)\cdots(2^n-2^{k-2})}{(k-2)!} & \text{if } 4 \leq k \leq n+1. \end{cases}$$

Moreover, the group of automorphisms of the design of indecomposable blocks is (isomorphic to) the group $\mathrm{GL}(n, 2)$ of invertible linear mappings on $\mathcal{P}$ over $\mathrm{GF}(2)$.

Finally, for $n \geq 4$ and $6 \leq k \leq 2^n - 4$, the family of decomposable blocks in $\mathcal{B}_k^*$ defines a 2-$(2^n - 1, k, \bar{\lambda})$ design, where

$$\bar{\lambda} = \begin{cases} \lambda & \text{if } k > n+1 \\ \lambda - \tilde{\lambda} & \text{if } 6 \leq k \leq n+1. \end{cases}$$

Proof. Let $\mathfrak{b} = \{P_1, \ldots, P_{k-1}, P_k = \sum_{j=1}^{k-1} P_j\}$ be an indecomposable block in $\mathcal{B}_k^*$. We claim that $P_1, \ldots, P_{k-1}$ are linearly independent. By contradiction, we may assume without loss of generality that $P_{k-1} = \sum_{j=1}^{k-2} \alpha_j P_j$, with $\alpha_j = 0, 1$, but not all zero. If each $\alpha_j = 1$, then $P_k = 0$, against the hypothesis that $\mathfrak{b} \in \mathcal{B}_k^*$. Therefore some $\alpha_j = 0$, whence $\mathfrak{b}$ is decomposable, a contradiction. Conversely, if $\mathfrak{b}$ contains $k-1$ linearly independent vectors, then all their possible sums are not zero, hence $\mathfrak{b}$ is indecomposable.

The formula for $\tilde{\lambda}$ follows then directly from a standard counting argument, or equivalently, it can be obtained from the fact that $\mathrm{GL}(n, 2)$ is 2-transitive on $\mathcal{P}^*$, and the family of indecomposable blocks in $\mathcal{B}_k^*$ consists of one single orbit under the action of $\mathrm{GL}(n, 2)$ on the k-subsets of $\mathcal{P}^*$.

As to the automorphism group, let φ be a permutation of $\mathcal{P}^*$. If φ is (the restriction to $\mathcal{P}^*$ of) an invertible linear mapping on $\mathcal{P}$ over GF(2), then it is immediate that φ maps the family of all indecomposable blocks in $\mathcal{B}_k^*$ onto itself. Conversely, assume that φ permutes the family of the indecomposable blocks in $\mathcal{B}_k^*$, and define $\varphi(0) = 0$. In order to prove that φ is a linear mapping on $\mathcal{P}$ over GF(2), it suffices to prove that

$$\varphi(x + y) = \varphi(x) + \varphi(y)$$

for all x, y in $\mathcal{P}^*$, with $x \neq y$. For $k = 3$, this is immediate, since $\{x, y, x + y\}$ is a (necessarily indecomposable) block in $\mathcal{B}_3^*$, hence so is $\{\varphi(x), \varphi(y), \varphi(x + y)\}$.

Let $k \geq 4$, and suppose, by contradiction, that there exist two distinct elements x, y in $\mathcal{P}^*$, such that $\varphi(x + y) \neq \varphi(x) + \varphi(y)$. Then the set $\{\varphi(x), \varphi(y), \varphi(x + y)\}$ contains three linearly independent vectors in $\mathcal{P}$, hence it is contained in a set $\{w_1, w_2, \ldots, w_{k-1}\}$ consisting of $k-1$ linearly independent vectors. Thus $\mathfrak{b} = \{w_1, w_2, \ldots, w_{k-1}, w_1 + \cdots + w_{k-1}\}$ is an indecomposable block in $\mathcal{B}_k^*$, and therefore so is $\varphi^{-1}(\mathfrak{b})$ by hypothesis, against the fact that the latter block contains $x, y, x + y$, which sum up to zero. This proves that φ is linear.

Finally, let $n \geq 4$ and $6 \leq k \leq 2^n - 4$. If $k > n + 1$, then all blocks in $\mathcal{B}_k^*$ are decomposable, since no block can contain $k - 1 > n$ linearly independent vectors. For $6 \leq k \leq n+1$, the family of decomposable blocks and the family of indecomposable blocks are both nonempty, and their union is all of $\mathcal{B}_k^*$. Hence the former family defines a 2-$(2^n - 1, k, \bar{\lambda})$ design, with $\bar{\lambda} = \lambda - \tilde{\lambda}$. □

2.10 Remark: In [10], [11] we found many additive 2-(v, k, λ) designs which could be embedded in a finite vector space V, in such a way that the blocks were characterized not only as the k-subsets $\{x_1, \ldots, x_k\}$ of V satisfying $x_1 + \cdots + x_k = 0$, but also as the intersections of the point-set of the design with suitable hyperplanes of V. Also in the present case we wish to find algebraic equations that describe the indecomposable blocks in the design $(\mathcal{P}^*, \mathcal{B}_k^*)$. This can be done because such blocks consist of a single orbit of the action of $\mathrm{GL}(n, 2)$ on $\binom{\mathcal{P}^*}{k}$. Let us start with the base block $\mathfrak{c}_k$ defined in Theorem 2.9.

Consider the sum $\sigma(x_1, \ldots, x_i)$ of the (nonconstant) elementary symmetric polynomials in $x_1, \ldots, x_i$, where each variable ranges in the field GF(2). Equivalently, $\sigma(x_1, \ldots, x_i) =$

$(1+x_1)\cdots(1+x_i)-1$, thus $\sigma(x_1,\ldots,x_i)=0$ if and only if $x_1=\ldots=x_i=0$. Also, let $\check{\sigma}_j(x_1,\ldots,x_i)=\sigma(x_1,\ldots,x_{j-1},x_{j+1},\ldots,x_i)$. Then

$$\begin{cases} x_1\cdots x_{k-1}+\sigma\Big(x_1\check{\sigma}_1(x_1,\ldots,x_{k-1}),\, x_2\,\check{\sigma}_2(x_1,\ldots,x_{k-1}),\ldots,\, x_{k-1}\check{\sigma}_{k-1}(x_1,\ldots,x_{k-1})\Big)=0 \\ x_k=0 \\ \vdots \\ x_n=0 \end{cases}$$

are algebraic equations whose set of solutions in $\mathcal{P}^*$ is precisely the k-set $\mathfrak{c}_k$. Indeed, let $(x_1,\ldots,x_n)$ be a solution in $\mathcal{P}^*$, say $x_i=1$ for some $1\le i\le k-1$. Thus

$$x_1\cdots x_{i-1}\,x_{i+1}\cdots x_{k-1}+\sigma\Big(x_1,\ldots,x_{i-1},\,\sigma(x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_{k-1}),\,x_{i+1},\ldots,\,x_{k-1}\Big)=0,$$

whence either $x_1=\ldots=x_{i-1}=x_{i+1}=\ldots=x_{k-1}=0$ or $x_1=\ldots=x_{i-1}=x_{i+1}=\ldots=x_{k-1}=1$, as claimed.

Also, for any matrix M in $\mathrm{GL}(n,2)$, the set of all $(x_1,\ldots,x_n)\in\mathcal{P}^*$, such that $M^{-1}(x_1,\ldots,x_n)'$ is a solution of the above system of equations, forms an indecomposable block in $\mathcal{B}_k^*$, and vice versa.

2.11 Remark: For $2\le k\le n$, the family $\mathcal{B}(k)$ of all the k-sets of linearly independent vectors of $\mathcal{P}^*$ defines a 2-$(2^n-1,k,\lambda)$ design, and it is readily seen directly that

$$\lambda=\begin{cases} 1 & \text{if } k=2 \\ \dfrac{(2^n-4)(2^n-8)\cdots(2^n-2^{k-1})}{(k-2)!} & \text{if } 3\le k\le n \end{cases}$$

(this again can be obtained from the fact that $\mathrm{GL}(n,2)$ is 2-transitive on $\mathcal{P}^*$, and $\mathcal{B}(k)$ consists of one single orbit under the action of $\mathrm{GL}(n,2)$ on the k-subsets of $\mathcal{P}^*$). Equivalently, $\mathcal{B}(k)$ consists of all the k-sets of elements of $\mathcal{P}^*$ that do not contain any subset belonging to $\mathcal{B}_h^*$ for any $h\le k$. Moreover, the group of automorphisms of the 2-design $(\mathcal{P}^*,\mathcal{B}(k))$ is (isomorphic to) the group $\mathrm{GL}(n,2)$ of invertible linear mappings on $\mathcal{P}$ over $\mathrm{GF}(2)$. The proof is similar to that given in the proof of Theorem 2.9 in the case of the 2-design of indecomposable blocks in $\mathcal{B}_k^*$.

3 Permutation automorphisms

In this final section we characterize the group of permutations of $\mathcal{P}$ (respectively, $\mathcal{P}^*$) inducing permutations of the "zero-sum subsets" of $\mathcal{P}$ (respectively, $\mathcal{P}^*$) of size k, essentially as a group of invertible linear mappings, and we apply these results to the cases of the automorphism groups of the binary Hamming code and of the extended binary Hamming code. Moreover, the permutation groups that we find in this section are also the automorphisms groups of the block designs introduced in Section 2.

We first consider the case of the permutations of $\mathcal{P}^*$ inducing permutations of $\mathcal{B}_k^*$, for a given k, with purely combinatorial arguments. As we point out below in Remark 3.5, in the different context of coding theory our result is (only implicitly) equivalent to the well known isomorphism between the permutation automorphism group of the binary Hamming code of length $m=2^n-1$ and the group $\mathrm{GL}(n,2)$, by virtue of some general results concerning perfect binary single-error correcting codes, which, in particular, are valid for binary Hamming codes.

3.1 Theorem: *Let $\mathcal{P}$ be an n-dimensional vector space over* GF(2), $n \geq 3$, *and, for a given $3 \leq k \leq 2^n - 4$, let $\mathcal{B}_k^*$ be the family of all the k-sets of elements of $\mathcal{P}^*$ adding up to zero. A permutation φ of $\mathcal{P}^*$ induces a permutation of $\mathcal{B}_k^*$ if and only if φ is (the restriction to $\mathcal{P}^*$ of) an invertible linear mapping on $\mathcal{P}$ over* GF(2).

Proof. Note first that $\mathcal{B}_k^*$ is not empty by Proposition 2.6. If φ is the restriction to $\mathcal{P}^*$ of an invertible linear mapping of $\mathcal{P}$ over GF(2), then

$$\sum_{x \in B} \varphi(x) = 0 \iff \sum_{x \in B} x = 0$$

for any k-set $B \subseteq \mathcal{P}^*$, that is, φ induces a permutation of $\mathcal{B}_k^*$.

Conversely, let φ be a permutation of $\mathcal{P}^*$ that induces a permutation of $\mathcal{B}_k^*$, and let us define $\varphi(0) = 0$. In order to prove that φ is a linear mapping on $\mathcal{P}$ over GF(2), it suffices to prove that

$$\varphi(x + y) = \varphi(x) + \varphi(y) \tag{9}$$

for all x, y in $\mathcal{P}^*$, with $x \neq y$. Up to taking complements, we can assume that $k < 2^{n-1}$.

If $k = 3$, then, for any $x \neq y$ in $\mathcal{P}^*$, the 3-set $\{x, y, x + y\}$ in $\mathcal{B}_3^*$ is mapped onto a 3-set of elements adding up to zero, that is, $\varphi(x) + \varphi(y) + \varphi(x + y) = 0$, hence $\varphi(x + y) = \varphi(x) + \varphi(y)$, as claimed.

If $k = 4$, then, for any $x \neq y$ in $\mathcal{P}^*$, the 4-set $\{0, x, y, x + y\}$ is a plane in $\mathcal{P}$, and $\mathcal{P}$ can be partitioned as

$$\mathcal{P} = \bigcup_{a \in S} \{a, a + x, a + y, a + x + y\},$$

for a suitable set $S \subseteq \mathcal{P}$. Since each 4-set $\{a, a+x, a+y, a+x+y\}$ different from $\{0, x, y, x+y\}$ belongs to $\mathcal{B}_4^*$, and since the sum of all the elements of $\mathcal{P}^*$ is equal to zero, we find that the set $\{\varphi(x), \varphi(y), \varphi(x + y)\}$ is complementary in $\mathcal{P}^*$ to a set of elements adding up to zero, that is, its elements add up to zero, as well, and it follows again that $\varphi(x + y) = \varphi(x) + \varphi(y)$.

Finally, assume that

$$4 < k < 2^{n-1}. \tag{10}$$

We claim that φ induces a permutation also on $\mathcal{B}_4^*$, thus the equality (9) follows from the case $k = 4$ above. Indeed, let $\{a, b, c, d\} \in \mathcal{B}_4^*$, and assume that there exist pairwise distinct elements $w_1, \ldots, w_{k-2}$ in $\mathcal{P}^*$, different from a, b, c, and d, such that $w_1 + \cdots + w_{k-2} = b + c$ $(= a + d)$. Therefore $\{b, c, w_1, \ldots, w_{k-2}\}$ and $\{a, d, w_1, \ldots, w_{k-2}\}$ are in $\mathcal{B}_k^*$, hence

$$\varphi(b) + \varphi(c) + \varphi(w_1) + \cdots + \varphi(w_{k-2}) = 0 = \varphi(a) + \varphi(d) + \varphi(w_1) + \cdots + \varphi(w_{k-2}),$$

thus $\varphi(a) + \varphi(b) + \varphi(c) + \varphi(d) = 0$, hence φ induces a permutation also on $\mathcal{B}_4^*$, as claimed.

In order to settle the existence of such vectors $w_1, \ldots, w_{k-2}$, we first notice that $a+b+c \neq 0$, thus a, b, c are linearly independent. Hence, up to an invertible linear mapping, we can assume that $a = e_1$, $b = e_2$, $c = e_3$, where e_1, e_2, e_3 are the first three vectors of the canonical basis of $\mathcal{P}$. Let $w_3, \ldots, w_{k-2}$ be any $k-4$ pairwise distinct vectors in $\mathcal{P}^* \setminus \{b, c\}$, with the property that their first coordinate is 0 and that the vector

$$w = b + c + w_3 + \cdots + w_{k-2}$$

is not equal to zero. Such vectors exist, since $2^{n-1} - 3 > k - 4$ by (10). Now, let w_1 be any vector not in $\{a, d, a + w, d + w\}$, with the property that its first coordinate be equal to 1 (the number of possible choices for w_1 is $2^{n-1} - 4$, which is positive by (10)). Finally, if we let $w_2 = w_1 + w$, then, by construction, $w_1, \ldots, w_{k-2}$ are pairwise distinct elements in $\mathcal{P}^* \setminus \{a, b, c, d\}$, and $w_1 + \cdots + w_{k-2} = w_1 + w_2 + (w + b + c) = b + c$, as required.

The proof is now complete. □

Next we consider the case of the permutations of $\mathcal{P}$ inducing permutations of $\mathcal{B}_k$. For k odd, the following result does not have an equivalent rephrasing in the frame of coding theory, since all codewords of the extended binary Hamming code have only even weights. For k even, an application to coding theory will be given in the subsequent Theorem 3.4.

3.2 Theorem: *Let $\mathcal{P}$ be an n-dimensional vector space over* GF(2) *and, for a given $3 \leq k \leq 2^n - 3$, let $\mathcal{B}_k$ be the family of all the k-sets of elements of $\mathcal{P}$ adding up to zero. If φ is a permutation of $\mathcal{P}$, then the following hold.*

i) In the case that k is odd, φ induces a permutation of $\mathcal{B}_k$ if and only if φ is an invertible linear map on $\mathcal{P}$ over GF(2).

ii) In the case that k is even, φ induces a permutation of $\mathcal{B}_k$ if and only if φ is an invertible affinity of the affine space $\mathcal{P}$ over the ground field GF(2), *that is, if and only if $\varphi(x) = \varphi_0(x) + \varphi(0)$, where φ_0 is an invertible linear map on $\mathcal{P}$ over* GF(2).

Proof. Note first that $\mathcal{B}_k$ is not empty by Theorem 2.2 and Proposition 2.5. Every invertible linear map on $\mathcal{P}$ permutes the elements of $\mathcal{P}$ and the k-sets in $\mathcal{B}_k$, and the same is true for invertible affinities, under the additional assumption that k is even.

Conversely, assume that φ induces a permutation of $\mathcal{B}_k$. We first show that we can reduce to the case where

$$\varphi(0) = 0.$$

If k is even, then it suffices to compose φ with the translation by $\varphi(0)$. If k is odd, then, as we noticed in the Remark 2.7.1 above, the number of k-sets in $\mathcal{B}_k$ containing 0 is different from the number of k-sets in $\mathcal{B}_k$ containing any other element y of $\mathcal{P}$. Since φ maps the k-sets in $\mathcal{B}_k$ containing 0 onto the k-sets in $\mathcal{B}_k$ containing $\varphi(0)$, it follows that $\varphi(0) = 0$, as claimed.

Mapping 0 to 0, φ induces a permutation of $\mathcal{P}^*$ which permutes the k-sets in $\mathcal{B}_k^*$, thus φ is linear, by Theorem 3.1, for all $3 \leq k \leq 2^n - 4$. If $k = 2^n - 3$, and φ permutes the k-sets in $\mathcal{B}_k$, then, by complementation, φ permutes also the 3-sets in $\mathcal{B}_3$; mapping 0 to 0, φ induces a permutation of $\mathcal{P}^*$ which permutes the 3-sets in $\mathcal{B}_3^*$, thus φ is linear by Theorem 3.1.

This completes the proof of the theorem. □

Last, but not least, we now derive, as another consequence of Theorems 3.1 and 3.2, one of the main results of this paper, that is, a characterization of the permutation automorphisms of the binary Hamming codes and of the extended binary Hamming codes.

Let us recall that a *permutation automorphism* of a code C is any permutation of the coordinate positions that maps codewords to codewords [19]. A permutation automorphism thus preserves each weight class of C. We will now prove that the converse is also true for just a given weight class in the case of binary Hamming codes: if the code has length $2^n - 1$, $n \geq 3$, and if k is a given weight different from $2^n - 1$ (hence necessarily such that $3 \leq k \leq 2^n - 4$), then

any permutation of the coordinate positions that maps codewords of weight k to codewords of weight k actually maps all codewords to codewords, hence is a permutation automorphism of the code. This allows one to relax the requirement in the definition of permutation automorphism of a binary Hamming code. Moreover, the following Theorem 3.3, together with Theorem 3.1, provides an alternative proof of the well known isomorphism between the permutation automorphism group of the binary Hamming code of length $m = 2^n - 1$ and the group $\mathrm{GL}(n, 2)$.

3.3 Theorem: (Characterization of the permutation automorphisms of binary Hamming codes) *Let C be a binary Hamming code of length $m = 2^n - 1$, $n \geq 3$, and let k be a given weight, with $3 \leq k \leq 2^n - 4$. If σ is a permutation of the m coordinate positions, then the following are equivalent.*

i) σ maps codewords to codewords, that is, σ is a permutation automorphism of C.

ii) σ maps codewords of weight k to codewords of weight k.

Proof. It suffices to prove that *ii)* $\Rightarrow$ *i)*. Let $3 \leq k \leq 2^n - 4$ be a given weight, let C_k be the set of all codewords of weight k, and let σ be a given permutation in the symmetric group S_m, which acts on $\mathrm{GF}(2)^m$ by

$$\sigma(x_1, x_2, \ldots, x_m) := (x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, \ldots, x_{\sigma^{-1}(m)}).$$

Suppose that $\sigma X \in C_k$ for all X in C_k. Let H be a parity check matrix for C, as at the beginning of Section 2, and recall that $\mathcal{P}^*$ is equal to the set $\{H^1, H^2, \ldots, H^m\}$ of the columns of H. Hence σ induces also a permutation $\tilde{\sigma}$ of $\mathcal{P}^*$ by

$$\tilde{\sigma} H^i = H^{\sigma(i)},$$

$i = 1, \ldots, m$. Finally, let $\theta : C_k \to \mathcal{B}_k^*$ be the invertible map defined in (1) (in particular, C_k is not empty by Proposition 2.6). Then $\theta\sigma\theta^{-1}$ maps $\mathcal{B}_k^*$ onto $\mathcal{B}_k^*$, and, by construction,

$$\theta\sigma\theta^{-1}\{H^{i_1}, H^{i_2}, \ldots, H^{i_k}\} = \{\tilde{\sigma}H^{i_1}, \tilde{\sigma}H^{i_2}, \ldots, \tilde{\sigma}H^{i_k}\}$$

for all $\{H^{i_1}, H^{i_2}, \ldots, H^{i_k}\}$ in $\mathcal{B}_k^*$. Equivalently, the induced action of $\tilde{\sigma}$ on $\mathcal{B}_k^*$ maps $\mathcal{B}_k^*$ onto $\mathcal{B}_k^*$, whence $\tilde{\sigma}$ is linear by Theorem 3.1. Therefore $\tilde{\sigma}$ maps $\mathcal{B}_h^*$ onto $\mathcal{B}_h^*$ for all weights $3 \leq h \leq 2^n - 4$, whence, by reversing the previous argument, σ maps C_h onto C_h for all weights $3 \leq h \leq 2^n - 4$. On the other hand, σ fixes trivially the zero codeword and the codeword of weight $2^n - 1$, hence σ maps all codewords in C to codewords in C, as claimed.

This completes the proof of the theorem. □

Similarly, by using the one-to-one correspondence $\bar{\theta}$ in (2) instead of θ, one proves the following result for the permutation automorphisms of the extended code, thereby providing, together with Theorem 3.2ii), an alternative proof of the well-known isomorphism between the permutation automorphism group of the extended binary Hamming code of length 2^n and the group $\mathrm{Aff}(n, 2)$ of invertible affine mappings on $\mathcal{P}$ over $\mathrm{GF}(2)$ (see, e.g., [24, Chapter 8]).

3.4 Theorem: (Characterization of the permutation automorphisms of extended binary Hamming codes) *Let $\bar{C}$ be an extended binary Hamming code of length 2^n, $n \geq 3$, and let k be a given (necessarily even) weight, with $4 \leq k \leq 2^n - 4$. If σ is a permutation of the 2^n coordinate positions, then the following are equivalent.*

i) σ maps codewords to codewords, that is, σ is a permutation automorphism of $\bar{C}$.

ii) σ maps codewords of weight k to codewords of weight k.

3.5 Remark: An alternative proof of Theorem 3.3 can be given by means of some general results concerning perfect binary single-error correcting codes, which, in particular, are valid for binary Hamming codes. Let us denote by $\mathrm{PAut}(C)$ (respectively, $\mathrm{PAut}(C_h)$) the set of all permutations of the m coordinate positions ($m = 2^n - 1$) that map codewords in C (resp., C_h) to codewords in C (resp., C_h), where h is any given weight. Then, by Corollary 1 in [2],

$$\mathrm{PAut}(C) \subseteq \mathrm{PAut}(C_k) \subseteq \mathrm{PAut}(C_3), \tag{11}$$

where $3 \leq k \leq 2^n - 4$ is a fixed weight. On the other hand, the set C_3 of codewords of weight 3 is a Steiner triple system, and

$$|\,\mathrm{PAut}(C_3)| \leq |\,\mathrm{GL}(n,2)| \tag{12}$$

by [27, Theorem 1]. Finally, it is well known that $\mathrm{PAut}(C)$ is isomorphic to $\mathrm{GL}(n,2)$ (see e.g. [24]; see [18] for the case of the general q-ary Hamming code), whence, by (11) and (12), $\mathrm{PAut}(C) = \mathrm{PAut}(C_k)$, as claimed.

Acknowledgements: The authors are grateful to Evgeniy V. Gorkunov for pointing out the articles [2] and [27], and to one of the anonymous referees for pointing out the articles [3] and [13].

References

[1] E. F. Assmus, Jr., On 2-ranks of Steiner triple systems, Electronic J. Combin. 2, article n. R9 (1995).

[2] S. V. Avgustinovich, A. Y. Vasil'eva, Reconstruction theorems for centered functions and perfect codes, Siberian Math. J. 49 (3), pp. 383-388 (2008).

[3] L. A. Bassalygo, V. A. Zinov'ev, A note on uniformly-packed codes (in Russian), Probl. Peredachi Inform. 13 (3), pp. 22-25 (1977).

[4] T. Beth, D. Jungnickel, H. Lenz, *Design theory*, 2nd ed., Cambridge University Press, Cambridge (1999).

[5] M. Braun, T. Etzion, P. R. J. Östergård, A. Vardy, A. Wassermann, On the existence of q-analogs of Steiner systems, Forum Math., Pi 4 (2016).

[6] M. Buratti, A. Del Fra, A lower bound on the number of Semi-Boolean quadruple systems, J. Comb. Des. 11, pp. 229-239 (2003).

[7] M. Buratti, A. Nakić, Designs over finite fields by difference methods, Finite Fields Appl. 57, pp. 128-138 (2019).

[8] M. Buratti, A. Nakić, A. Wassermann, Graph decompositions over projective geometries, J. Combin. Des. 29, pp. 149-174 (2021).

[9] A. Caggegi, Some additive 2-$(v, 5, \lambda)$ designs, Acta Univ. Palacki. Olomuc., Fac. Rerum Nat., Math. 54, pp. 65-80 (2015).

[10] A. Caggegi, G. Falcone, M. Pavone, On the additivity of block designs, J. Algebr. Comb. 45, pp. 271-294 (2017).

[11] A. Caggegi, G. Falcone, M. Pavone, Additivity of affine designs, J. Algebr. Comb. (2020), DOI: 10.1007/s10801-020-00941-8.

[12] C. J. Colbourn, J. H. Dinitz, *The CRC Handbook of Combinatorial Designs*, 2nd ed., CRC Press, Boca Raton (2007).

[13] P. Delsarte, Four fundamental parameters of a code and their combinatorial significance, Inf. Control 23 (5), pp. 407-438 (1973).

[14] T. Etzion, A. Vardy, Perfect Binary Codes: Constructions, Properties, and Enumeration, IEEE Trans. Inf. Theory 40 (3), pp. 754-763 (1994).

[15] G. Falcone, M. Pavone, Kirkman's Tetrahedron and the Fifteen Schoolgirl Problem, Amer. Math. Month. 118 (10), pp. 887-900 (2011).

[16] G. Falcone, M. Pavone, Permutations of zero-sumsets in a finite vector space, Forum Math. (2020), DOI: 10.1515/forum-2019-0228.

[17] N. Gill, N. I. Gillespie, C. E. Praeger, J. Semeraro, Conway's groupoid and its relatives, in: *Finite Simple Groups: Thirty Years of the Atlas and Beyond*, Contemporary Mathematics, Vol. 694, American Mathematical Society, pp. 91-110 (2017).

[18] E. V. Gorkunov, The group of permutation automorphisms of a q-ary Hamming code, Probl. Inf. Transm. 45, pp. 309-316 (2009).

[19] W. C. Huffman, Codes and groups, in: V. S. Pless and W. C. Huffman, editors, *Handbook of Coding Theory*, pp. 1345-1440, Elsevier, Amsterdam (1998).

[20] J. D. Key, F. E. Sullivan, Steiner systems from binary codes, Ars Comb. 52, pp. 153-159 (1999).

[21] M. Kosters, The subset sum problem for finite abelian groups, J. Combin. Theory, Ser. A 120 (3), pp. 527-530 (2013).

[22] J. Li, D. Wan, On the subset sum problem over finite fields, Finite Fields Appl. 14 (4), pp. 911-929 (2008).

[23] J. Li, D. Wan, Counting subset sums of finite abelian groups, J. Combin. Theory, Ser. A 119 (1), pp. 170-182 (2012).

[24] F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, New York (1977).

[25] M. Pavone, Subset sums and block designs in a finite vector space (submitted).

[26] J. R. Schatz, On the Weight Distributions of Cosets of a Linear Code, Amer. Math. Monthly 87 (7), pp. 548-551 (1980).

[27] F. I. Solov'eva, S. T. Topalova, On Automorphism Groups of Perfect Binary Codes and Steiner Triple Systems (in Russian), Probl. Peredachi Inf. 36 (4), pp. 53-58 (2000).

[28] S. Thomas, Designs over finite fields, Geom. Dedic. 93, pp. 237-242 (1987).

[29] V. D. Tonchev, A formula for the number of Steiner quadruple systems on 2^n points of 2-rank $2^n - n$, J. Comb. Des. 11, pp. 260-274 (2003).